

(19)



JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **09307542 A**

(43) Date of publication of application: 28 . 11 . 97

(51) Int. Cl.

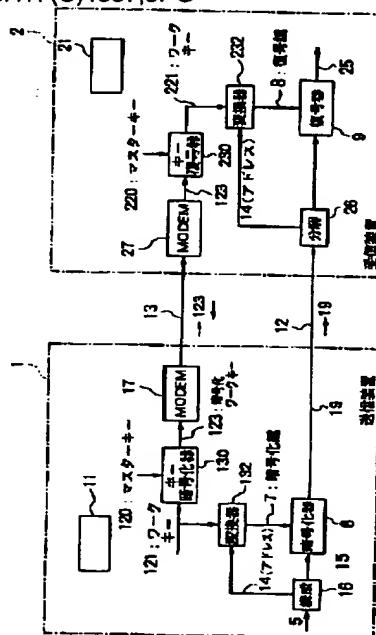
H04L 9/08
G09C 1/00
(21) Application number: **08154688**(22) Date of filing: **14 . 06 . 96**(30) Priority: **15 . 03 . 96 JP 08 59746**(71) Applicant: **SONY CORP**
(72) Inventor:
ASANO TOMOYUKI
ISHII MAKOTO
KUBOTA ICHIRO
(54) DATA TRANSMITTER AND DATA TRANSMISSION METHOD
(57) Abstract:

PROBLEM TO BE SOLVED: To enhance the security against leakage of ciphered transmission data by improving the security of transmission of a ciphering key or a decoding key.

SOLUTION: A large capacity transmission channel 12 such as a satellite transmission channel through which data of a large capacity are transmitted and a small capacity transmission channel 13 such as a public telephone line to send a ciphering key or a decoding key are provided. A ciphering session key is converted by using a work key and a destination address of a receiver 2 being a transmission destination. Furthermore, a decoding session key is converted by using its own address and the work key. The work key is preferably ciphered and sent through the small capacity transmission line 13. A transmitter 1 ciphers data 5 to be transmitted by using the converted ciphering session key 7 as above and adds transmission control information such as destination data to the data 5 and the resulting data 5 are sent to a receiver 2 through the large capacity transmission channel 12. The receiver 2 uses a decoding session key 8

converted as above to decode ciphered data 19.

COPYRIGHT: (C)1997,JPO



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-307542

(43) 公開日 平成9年(1997)11月28日

(51) Int.Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L 9/08			H 0 4 L 9/00	6 0 1 B
G 0 9 C 1/00	6 3 0	7259-5 J	G 0 9 C 1/00	6 3 0 B
		7259-5 J		6 3 0 E
			H 0 4 L 9/00	6 0 1 E

審査請求 未請求 請求項の数 8 O L (全 16 頁)

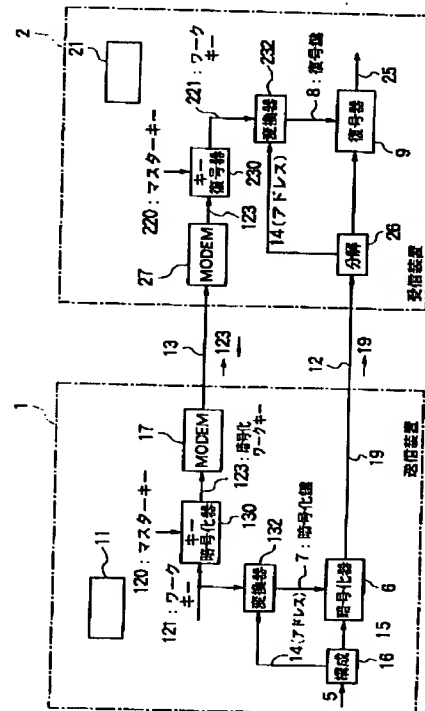
(21) 出願番号	特願平8-154688	(71) 出願人	000002185 ソニー株式会社 東京都品川区北品川6丁目7番35号
(22) 出願日	平成8年(1996)6月14日	(72) 発明者	浅野 智之 東京都品川区北品川6丁目7番35号 ソニー株式会社内
(31) 優先権主張番号	特願平8-59746	(72) 発明者	石井 眞 東京都品川区北品川6丁目7番35号 ソニー株式会社内
(32) 優先日	平8(1996)3月15日	(72) 発明者	窪田 一郎 東京都品川区北品川6丁目7番35号 ソニー株式会社内
(33) 優先権主張国	日本 (J P)	(74) 代理人	弁理士 佐藤 隆久

(54) 【発明の名称】 データ伝送装置とその方法

(57) 【要約】

【課題】 暗号鍵または復号鍵の伝送の安全性を高め、暗号化伝送データの漏洩に対する安全性を高めるデータ伝送装置を提供する。

【解決手段】 大容量のデータを伝送する衛星回線伝送路などの大容量伝送路12と、暗号鍵または復号鍵あるいはこれらの生成のための情報を伝送する公衆電話回線などの小容量伝送路13を設ける。暗号化セッション鍵をワークキーと送信先の受信装置2の宛先アドレスとを用いて変換する。また復号用セッション鍵を自己のアドレスとワークキーを用いて変換する。ワークキーは好ましくは、暗号化されて小容量伝送路13を伝送される。送信装置1において、伝送すべきデータ5を上記のごとく変換した暗号セッション7を用いて暗号化する他、宛先データなどの伝送制御情報を付加して大容量伝送路12を経由して受信装置2に伝送する。受信装置2において、上記のごとく変換した復号セッション鍵8を用いて暗号化データ19を復号する。



【特許請求の範囲】

【請求項1】大量のデータを高速で伝送可能な第1の伝送系統と、

有線形式の第2の伝送系統と、

前記第1の伝送系統と前記第2の伝送系統を介して接続されている第1の伝送装置と第2の伝送装置とを有し、前記第1の伝送装置が前記第2の伝送系統を介して復号化セッション鍵を生成するためのワークキーを前記第2の伝送装置に伝送し、

前記第1の伝送装置が、暗号化データを送信する前記第2の伝送装置の宛先データおよび前記暗号化セッション鍵を生成するためのワークキーを用いて暗号化セッション鍵を生成し、該生成した暗号化セッション鍵を用いて伝送データを暗号化し、前記宛先データを付加して前記第1の伝送系統に送出し、

前記第2の伝送装置は前記第1の伝送系統から受信したデータから前記宛先データを取り出し、該宛先データと前記第2の伝送系統から受信した暗号化セッション鍵を生成するためのワークキーとから復号化セッション鍵を生成し、該生成した復号化セッション鍵を用いて前記暗号化伝送データを復号するデータ伝送装置。

【請求項2】前記宛先アドレスは複数の装置のグループを示すアドレスである、請求項1記載のデータ伝送装置。

【請求項3】前記第1の伝送系統は衛星回線伝送路である、請求項1または2記載のデータ伝送装置。

【請求項4】前記第1の伝送装置は、前記第2の伝送系統を介して前記第2の伝送装置に伝送する、復号化セッション鍵を生成するためのワークキーを暗号化して伝送し、

前記第2の伝送装置は、該暗号化されている復号化セッション鍵を生成するためのワークキーを復号し、該復号したワークキーと前記宛先データを用いて復号化セッション鍵を生成する請求項1～3いずれか記載のデータ伝送装置。

【請求項5】大量のデータを高速で伝送可能な第1の伝送系統および有線形式の第2の伝送系統に接続され、ワークキーを前記第2の伝送系統に送出する第1の送出手段と、

ワークキーと送信先のアドレスとから暗号化セッション鍵を生成する鍵変換手段と、

前記生成した暗号化セッション鍵を用いて伝送すべきデータを暗号化するデータ暗号化手段と、

該暗号化伝送データに、送信先のアドレスを付加して前記第1の伝送系統に送出する送出手段とを有するデータ伝送装置。

【請求項6】大量のデータを高速で伝送可能な第1の伝送系統と、有線形式の第2の伝送系統とを用いて第1の伝送装置と第2の伝送装置との間で暗号化データを伝送するデータ伝送方法であって、

前記第2の伝送系統を介して復号化セッション鍵を生成するためのワークキーを前記第2の伝送装置に伝送し、暗号化データを送信する前記第2の伝送装置の宛先データおよび前記暗号化セッション鍵を生成するためのワークキーを用いて暗号化セッション鍵を生成し、該生成した暗号化セッション鍵を用いて伝送データを暗号化し、前記宛先データを付加して前記第1の伝送系統に送出し、

前記第1の伝送系統から受信したデータから前記宛先データを取り出し、該宛先データと前記第2の伝送系統から受信した暗号化セッション鍵を生成するためのワークキーとから復号化セッション鍵を生成し、該生成した復号化セッション鍵を用いて前記暗号化伝送データを復号するデータ伝送方法。

【請求項7】前記宛先アドレスは複数の装置のグループに対するアドレスである、請求項6記載のデータ伝送方法。

【請求項8】大量のデータを高速で伝送可能な第1の伝送系統と、

有線形式の第2の伝送系統と、

前記第1の伝送系統と前記第2の伝送系統を介して接続されている第1の伝送装置と第2の伝送装置とを有し、前記第1の伝送装置が前記第2の伝送系統を介して復号化セッション鍵を生成するためのワークキーを前記第2の伝送装置に伝送し、

前記第1の伝送装置が、前記暗号化セッション鍵を生成するためのワークキーを用いて暗号化セッション鍵を生成し、該生成した暗号化セッション鍵を用いて伝送データを暗号化し、前記宛先データを付加して前記第1の伝送系統に送出し、

前記第2の伝送装置は前記第2の伝送系統から受信した暗号化セッション鍵を生成するためのワークキーとから復号化セッション鍵を生成し、該生成した復号化セッション鍵を用いて前記暗号化伝送データを復号するデータ伝送装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はデータを伝送するデータ伝送装置とその方法に関するものであり、特に、大量のデータを暗号化して送受信する場合に用いる暗号鍵および復号鍵の管理を適切に行うデータ伝送装置とその方法に関する。

【0002】

【従来の技術】公衆電話回線、専用回線などを用いてデータ伝送する場合または通話する場合、伝送情報の漏洩を防止するためまたは伝送情報に対する攻撃（妨害）に対して情報の信頼性を維持するため、平文のデータを暗号化し（スクランブルし）て伝送し、受信先で暗号化されたデータを復号して（デスクランブルして）いる。代表的な暗号方式としては共通鍵暗号方式と公開鍵方式と

が知られている。共通鍵暗号方式は対称暗号系とも呼ばれており、アルゴリズム非公開型とアルゴリズム公開型とが知られている。アルゴリズム公開型の代表的なものとしてDES (Data Encryption Standard) が知られている。公開鍵方式は、検査鍵から生成鍵を導出するために莫大な計算量が必要なため実質的に生成鍵が解読されないので、暗号鍵を公開してもよい暗号方式であり、非対称鍵暗号方式とも呼ばれている。

【0003】暗号化方式は伝送データが伝送される回線系統の種別、伝送データの機密度（秘密性）、伝送データの量などに応じて決定される。専用回線を用いたデータ伝送においては、情報の漏洩、伝送データへの攻撃の度合いは低い、公衆電話回線を用いてデータ伝送する場合は情報の漏洩の度合い、攻撃の度合いは高くなる。さらに衛星放送回線を用いたデータ伝送は、不特定多数の装置で受信可能であるから情報の漏洩の度合いは一層高くなる。

【0004】図1は伝送路上のデータを共通鍵暗号化方式で暗号化する暗号化データ伝送装置の一例を示す概略構成図である。図1の暗号化データ伝送装置において、符号1は送信装置（送信者）を示し、2は受信装置（受信者）を示し、3は盗聴装置（盗聴者）を示し、4はデータ伝送路を示し、5は伝送すべきデータを示し、6は送信装置1内に設けられた暗号化器を示し、7は暗号化器6で暗号化に用いる暗号化鍵（暗号化用セッションキーという）を示し、8は復号鍵（復号用セッションキーという）を示し、9は復号鍵を用いてデータ伝送路4から受信した暗号化データを復号する復号器を示し、10は復号後のデータを示す。送信装置1において、データ5を伝送路4上に送出する際に、暗号化器6において暗号化鍵7を用いてデータ5を暗号化し、暗号化したデータを伝送路4を経由して受信装置2に送出する。受信装置2において、伝送路4から暗号化されたデータを受信したら、復号器9において暗号化鍵7に対応する復号鍵8を用いて受信した暗号化されたデータを復号し、目的とする復号（解読）データ10を得る。この例においては、盗聴装置3が伝送路4から受信装置2と同様に暗号化されたデータを受信しても、復号鍵8がないのでこれを正しく復号することが困難である。すなわち、盗聴装置3ではそのままでは意味不明のスクランブルのかかったデータを扱うことになるから、現実的に盗聴装置3側に情報が漏洩することを防いでいる。この例における共通鍵暗号方式の主要な暗号化方式では、一般に暗号化鍵と復号鍵は同一のビット列である。

【0005】最近、特定の契約者との間にのみTV番組を提供する衛星放送が行われている。衛星放送に用いる伝送系統は、映像と音声という大量のデータ（情報）を短時間で伝送することが可能である。また人工衛星を用いた伝送系統は、大量の情報を短い時間で伝送することが可能であるため、放送に限らず、コンピュータ・デー

タなどのデータの伝送に広く利用されている。しかしながら、人工衛星を用いた伝送においては、電話回線、専用回線などの1対1通信方式と異なり、不特定多数の多くの受信者が（受信装置で）容易に受信できるので、盗聴されやすいという面も有している。その結果、たとえば、有料衛星放送が盗聴される可能性が高い。そこで、TV放送の映像データ、音声データについても暗号化して伝送することが提案されている。実際の伝送においては全てのデータについて暗号化処理をする訳ではなく、送信装置において伝送すべきデータの内容に応じて、暗号化すべきデータを暗号化して伝送路上に送出し、受信者は暗号化されたデータの全部または一部を復号し、その結果得られた情報により、現在その全部または一部が復号されたデータが自分にとって必要なものであるか否かを知る。

【0006】このように暗号化したデータを伝送する暗号化データ伝送装置において、送信側と受信側とで、事前に暗号鍵と復号鍵を秘密に持つ必要がある。送信側で暗号鍵を持ち受信側で復号鍵を持つ従来の方法としては、たとえば、衛星回線伝送路を用いて映像データなどを暗号化して伝送する場合には、送信者が受信者に復号鍵を記録した紙やICカード等を郵送等の方法で送る方法と、衛星回線伝送路を暗号鍵と復号鍵を伝送する方法、さらにこれらを組み合わせた方法が考えられる。

【0007】

【発明が解決しようとする課題】暗号鍵と復号鍵の従来の管理方法には下記に挙げる問題がある。第1の問題は、送信者による暗号化鍵の所有のしかた、あるいは受信者による復号鍵の所有のしかたに関係した問題である。上述したように、送信者が暗号化鍵を持ち受信者が復号鍵を持つための方法としては、送信者が受信者に復号鍵を記録した紙、ICカードなどの物体を郵送等の方法で送る方法と、衛星回線伝送路を用いて送る方法、さらにこれらを組み合わせた方法が一般的である。

(1) 復号鍵を記録した物体を郵送等で送る方法においては、その手続きの繁雑さから暗号化鍵および復号鍵の変更が容易に行えない。そのため多くのデータに対して同一の鍵を用いて暗号化したデータを伝送路上に送出することになり、盗聴者により多くの情報を与えるという意味で、暗号解読に対しての安全性が低い。

(2) 復号鍵を衛星回線伝送路を用いて送る方法においては、衛星回線伝送路上のデータは、その者を送信者が受信者として希望するか否かにかかわらず、アンテナ等の機材を持つ不特定多数の者に受信されることから、送信者が希望する受信者以外の者に復号鍵を知られてしまう可能性があるため、伝送の安全が保てないという課題がある。

(3) 上記2つの方法を組み合わせる方法、つまり、郵送等で送られた物体に記録してある情報と、衛星回線伝送路を伝送された情報から復号鍵を作成する方法におい

ては、2つの方法の欠点が補われ、この伝送方法の安全性はある程度強いものになる。しかし、たとえば、衛星回線伝送路上のデータを受信でき、かつ、郵送等で他人に送られた情報をなんらかの方法で知りえた者は、この他人が用いる復号鍵を知り、暗号化されている衛星回線伝送路上の他人宛のデータの復号ができることになり、依然として情報が漏洩するという問題がある。

【0008】第2の問題は送信者がデータを暗号化するか否かを、あるいは、受信者が受信したデータを復号するか否かをいかにして判断するかに関する。上述したように、現在一般的に用いられている方法では、送信装置においてデータの内容を見て暗号化する必要のあるデータを暗号化して伝送路上に送信し、受信装置においては伝送路から受信した暗号化されたデータの全部または一部を復号して得られた情報により、このデータが自分にとって必要であるか否かを判断する。しかしこの方法では、送信装置において、データが暗号化する必要のあるものか否かを知るためにその内容を知るための処理と、受信装置において受信した暗号化されたデータは自分の必要とするものであるか否かを判断するために暗号化されたデータの全部または一部を復号するための処理が必要である。そのためにはより高速に伝送を行う必要があるが、これまでの装置構成ではその要望を満足できなかった。

【0009】本発明の目的は、送信側において有効に伝送データを暗号化し、受信側において伝送された暗号化データを有効に復号できるデータ伝送装置とその方法を提供することにある。

【0010】

【課題を解決するための手段】本発明においては、送信側が、ワークキーとを用いて暗号化セッション鍵を生成する、好適には、受信側の宛先アドレスとワークキーとを用いて暗号化セッション鍵を生成して、その鍵を用いて伝送データを暗号化して、第1の伝送系統を介して送出する。送信側から受信側に第2の伝送系統を介してワークキーを伝送しておく。受信側では、ワークキーを用いて、または好適には宛先アドレスとワークキーとを用いて復号化セッション鍵を生成し、この鍵を用いて伝送データを復号する。本発明は、第2の課題を解決するために、送信者がデータを暗号化するか否かを、あるいは、受信者が受信したデータを復号するか否かを、データを伝送するための制御情報によって判断する。本発明においては、大量のデータを高速かつ効率よく伝送可能な衛星放送伝送系統（伝送路）などの大容量伝送路（第1の伝送系統）と、この大容量伝送路とは独立に、ワークキーの授受を行う公衆電話回線などの小容量伝送路（第2の伝送系統）を用いる。小容量伝送路としては、漏洩に対する機密性を高めるため、送信装置と受信装置との間の通信が1対1で行える有線通信路が好ましい。

【0011】したがって、本発明によれば、大量のデー

タを高速で伝送可能な第1の伝送系統と、有線形式の第2の伝送系統と、第1の伝送系統と第2の伝送系統を介して接続されている第1の伝送装置と第2の伝送装置とを有し、第1の伝送装置が第2の伝送系統を介して復号化セッション鍵を生成するためのワークキーを第2の伝送装置に伝送し、第1の伝送装置が、暗号化データを送信する第2の伝送装置の宛先データおよび前記暗号化セッション鍵を生成するためのワークキーを用いて暗号化セッション鍵を生成し、該生成した暗号化セッション鍵を用いて伝送データを暗号化し、宛先データを付加して第1の伝送系統に送出し、第2の伝送装置は第1の伝送系統から受信したデータから宛先データを取り出し、該宛先データと第2の伝送系統から受信した暗号化セッション鍵を生成するためのワークキーとから復号化セッション鍵を生成し、該生成した復号化セッション鍵を用いて暗号化伝送データを復号するデータ伝送装置が提供される。宛先アドレスとしては、単一の装置を示す場合に限らず、複数の装置のグループを示すこともできる。

【0012】好適には、第1の伝送系統は衛星回線伝送路である。また好適には、第1の伝送装置は、第2の伝送系統を介して第2の伝送装置に伝送する、復号化セッション鍵を生成するためのワークキーを暗号化して伝送し、第2の伝送装置は、該暗号化されている復号化セッション鍵を生成するためのワークキーを復号し、該復号したワークキーと前記宛先データを用いて復号化セッション鍵を生成する。

【0013】また本発明によれば、大量のデータを高速で伝送可能な第1の伝送系統および有線形式の第2の伝送系統に接続され、ワークキーを第2の伝送系統に送出する第1の送出手段と、ワークキーと送信先のアドレスとから暗号化セッション鍵を生成する鍵変換手段と、生成した暗号化セッション鍵を用いて伝送すべきデータを暗号化するデータ暗号化手段と、該暗号化伝送データに、送信先のアドレスを付加して第1の伝送系統に送出する送出手段とを有するデータ伝送装置が提供される。

【0014】さらに本発明によれば、大量のデータを高速で伝送可能な第1の伝送系統と、有線形式の第2の伝送系統とを用いて第1の伝送装置と第2の伝送装置との間で暗号化データを伝送するデータ伝送方法であって、第2の伝送系統を介して復号化セッション鍵を生成するためのワークキーを第2の伝送装置に伝送し、暗号化データを送信する第2の伝送装置の宛先データおよび暗号化セッション鍵を生成するためのワークキーを用いて暗号化セッションキー鍵を生成し、該生成した暗号化セッション鍵を用いて伝送データを暗号化し、宛先データを付加して第1の伝送系統に送出し、第1の伝送系統から受信したデータから宛先データを取り出し、該宛先データと第2の伝送系統から受信した暗号化セッション鍵を生成するためのワークキーとから復号化セッション鍵を生成し、該生成した復号化セッション鍵を用いて暗号化

伝送データを復号する、データ伝送方法が提供される。

【0015】

【発明の実施の形態】

【実施例1】本発明のデータ伝送装置の第1実施例について、図2を参照して述べる。図2は本発明のデータ伝送装置の第1実施例の概念的な構成図である。図2に図解した第1実施例のデータ伝送装置において、符号1は送信装置（送信者、または第1の伝送装置）を示し、2は受信装置（受信者または第2の伝送装置）を示し、3は送信装置1および受信装置2を除く第3者の受信装置を示し、12は第1の伝送システムとしての大容量伝送路を示し、13は第2の伝送システムとしての小容量伝送路を示す。

【0016】本発明においては、大容量伝送路12を介してTV信号、コンピュータデータなどの大量のデータを伝送する。大容量伝送路12としては、大量のデータを高速かつ効率よく伝送する衛星回線伝送路が好ましい。また、暗号または復号に関する情報を伝送する小容量伝送路13としては、衛星回線伝送路より情報の漏洩が少ない1対1通信を行う、有線伝送路、たとえば、公衆電話回線、専用回線などが望ましい。以下の実施例においては、小容量伝送路13として公衆電話回線を用いた場合を例示する。

【0017】図3は大容量伝送路12として衛星回線伝送路を用い、小容量伝送路13として公衆電話回線を用いた伝送路の概略構成を示す図である。衛星回線伝送路12は、送信用アンテナ120、空中伝送路121、中継器を内蔵した人工衛星122、空中伝送路123、および、受信用アンテナ124から構成されている。送信用アンテナ120には、送信装置1に設けられた送信機（TX）10が接続され、受信用アンテナ124には受信装置2に設けられた受信機（RX）20が接続されている。受信機20としては、たとえば、TV映像信号を受信する場合は、TV受像機内の受信機である。なお、アンテナ120、124は送信用だけでなく受信用にも用いることができる。送信装置1内の送信機（TX）10、受信装置2内の受信機（RX）20はそれぞれ送受信機として、送信も受信も可能な装置を設けることができる。特に、大容量伝送データとして、コンピュータデータを伝送する場合などは、相互に送受信する場合が多いから、送信装置1および受信装置2にそれぞれ送受信機を設けておくことが望ましい。公衆電話回線13は、送信装置1内に変復調器（MODEM：モデム）17を設け、受信装置2内にも変復調器（モデム）27を設けておき、これら変復調器17、27相互で、電話線131、交換機（EX）130、電話線132を介して暗号鍵などのデータの伝送を行う。以下、大容量伝送路12としては、図3に図解した衛星回線伝送路12、小容量伝送路13として図3に示した公衆電話回線13を例示する。

【0018】送信装置1が大容量伝送路12に送出した暗号化したデータを、大容量伝送路12と無線接続されている受信装置2に送信する。本実施例においては、送信装置1は大容量伝送路12を用いて、伝送すべきデータをインターネット・プロトコル（INTERNET Protocol：インターネット通信規約）IPを用いて伝送する。なお通信規約としては、インターネット・プロトコルIPに限らず、後述するように、たとえば、ATM（Asynchronous Transfer Mode、非同期転送モード）など、その他の通信規約を用いることもできる。ただし、以下の実施例においては、インターネット・プロトコルIPについて例示する。インターネット・プロトコルIPは、データの伝送における代表的なプロトコルであり、その詳細はたとえば、西田竹志著の文献、TCP/IP インターネットワークング、株式会社、ソフト・リサーチ・センター発行、に示されている。

【0019】図4はインターネット・プロトコルIPにおけるメッセージ伝送の単位であるIPデータグラム15の概略図である。符号5は伝送すべきデータを示し、14はIPヘッダを示し、15はメッセージ伝送の1単位であるIPデータグラムを示す。インターネット・プロトコルIPに従えば伝送すべきデータ5に、伝送に必要な制御情報であるIPヘッダ14が付加され、全体がIPデータグラム15を構成する。本実施例においては、IPヘッダ14には、送信装置1からデータを伝送する宛先データ（すなわち、受信装置2の宛先データ）、および、伝送すべきデータ5を暗号化するか否かのフラグがセットされる。IPヘッダ14に規定される宛先データおよび暗号化するか否かの情報を伝送制御情報と呼ぶ。

【0020】データ伝送装置の構成

図5は図2に図解した本発明の暗号化データ伝送装置の第1実施例についてインターネット・プロトコルIPを適用して実現したより詳細な構成を示す図である。暗号化データ伝送装置は、大容量伝送路12（具体的には、図3に図解した大容量伝送路12）と小容量伝送路13（具体的には、図3に図解した公衆電話回線13）を介して接続されている送信装置1と受信装置2とを有している。送信装置1には、図4に図解したように伝送すべきデータ5にIPヘッダ14を付加してIPデータグラム15を形成するIPデータグラム構成器16と、暗号鍵7を用いてIPデータグラム15を暗号化して暗号化データ19を生成する暗号化器6が設けられている。衛星回線伝送路12には、図示しない送信機10（図3参照）を用いて暗号化器6で暗号化された暗号化データ19とIPデータグラム構成器16から出力されて暗号化されていない平文データ18とが伝送される。送信装置1にはさらに、公衆電話回線13を介して復号鍵の伝送を行う変復調器（モデム）17と、送信装置1内の信号処理および制御処理を行う信号処理装置11とが設けら

れている。信号処理装置 11 は、たとえば、コンピュータを用いて構成されている。信号処理装置 11 は IP データグラム構成器 16、暗号化器 6 および変復調器（モデム）17 の全体処理および制御を行う。受信装置 2 には、データグラム分解器 26、復号器 9、信号処理装置 21、変復調器（モデム）27 が設けられている。

【0021】送信装置 1 の動作

送信装置 1 において、IP データグラム構成器 16 が伝送すべきデータ 5 に IP ヘッダ 14 を付加して IP データグラム 15 を生成する。この際に、送信装置 1 の信号処理装置 11 は IP ヘッダ 14 中の宛先アドレスの部分を用いて、伝送データ 5 を暗号化するか否かを判断し、暗号化する場合、ハードウェアとして構成された暗号化器 6 を用いて暗号化鍵（暗号化用セッションキー）7 を鍵として伝送すべきデータ 5 を暗号化し、暗号化データ 19 を衛星回線伝送路 12 に送出する。なお、暗号鍵 7 は、送信装置 1 内の信号処理装置 11 が上記宛先アドレスに基づいて生成する。伝送データ 5 を暗号化しない場合には、送信装置 1 は暗号化されていない IP データグラム（平文データ）18 を衛星回線伝送路 12 に送出する。

【0022】図 6 は、上記の送信装置の主要な処理の流れを示すフローチャートである。ステップ S1 において送信装置 1 の IP データグラム構成器 16 は伝送すべきデータ 5 に IP ヘッダを付加して IP データグラムを生成する。ステップ S2 において、送信装置 1 の暗号化器 6 は IP ヘッダ 14 に含まれる宛先アドレスを見てデータを暗号化するか否かを判断する。暗号化する場合、ステップ S3 へ進み、暗号化器 6 は暗号鍵 7 を用いて伝送すべきデータ 5 に対して暗号化処理を行う。その後、ステップ S4 へ進み、送信装置 1 の送信機 10（図示せず）は暗号化したデータを衛星回線伝送路 12 に送出する。暗号化しない場合には、ステップ S4 に進み、送信装置 1 の送信機 10（図示せず、図 3 参照）は暗号化しない平文データ 18 を衛星回線伝送路 12 に送出する。信号処理装置 11 はこれらの動作処理および制御を行う。

【0023】復号鍵 8 の伝送

衛星回線伝送路 12 を用いたデータの伝送とは別に、公衆電話回線 13 を用いて、信号処理装置 11 と変復調器（モデム）17、および、信号処理装置 21 と変復調器（モデム）27 との間で、送信装置 1 から受信装置 2 に暗号鍵 7 に対応する復号鍵 8 を伝送しておく。これにより、暗号鍵 7 に対応した復号鍵 8 を用いれば受信装置 2 において暗号化データ 19 の復号が可能になる。

【0024】受信装置 2 の動作

受信装置 2 において、図示しない受信機 20（図 3 参照）で衛星回線伝送路 12 から受信した、平文データ 18 および暗号化データ 19 を IP データグラム分解器 26 に入力する。IP データグラム分解器 26 は、受信デ

ータから IP ヘッダ 14 を分離し、この中の宛先アドレスを見て、このデータが自分宛のものか否かと、復号すべきか否かを調べる。このデータが自分宛のものである場合には、IP データグラム分解器 26 は IP ヘッダ 14 を除いた受信データ 29 を後段の回路、たとえば、暗号化データについては復号器 9、および、平文データについては図示しない回路に送出する。復号すべき場合には、ハードウェアとして構成されている復号器 9 が復号鍵（復号用セッションキー）8 を用いて、IP ヘッダ 14 を分離した後の暗号化データ 29 を、送信装置 1 における伝送すべきデータ 5 に相当するもとのデータ 25 に復号する。衛星回線伝送路 12 から受信したデータが自分宛のものであり、復号する必要のない平文である場合には、IP データグラム分解器 26 は IP ヘッダ 14 を分離し、その後、復号鍵を用いて復号することなく、平文データ 28 として送信装置 1 における伝送すべきデータ 5 に相当するもとの送信データを取り出す。

【0025】図 7 は図 5 に示した受信装置 2 における動作処理の流れを示すフローチャートである。ステップ S5 で、受信装置 2 の IP データグラム分解器 26 は図示しない受信機（図 3 参照）で受信した平文データ 18 および暗号化データ 19 の IP データグラム 15 から IP ヘッダ 14 を取り出す。平文データ 18 から IP ヘッダ 14 を除いてデータを平文データ 28 とし、暗号化データ 19 から IP ヘッダ 14 を除いてデータを暗号化データ 29 とする。ステップ S6 で、信号処理装置 21 は IP ヘッダ 14 の宛先アドレスを見て自分宛のデータであるかどうか判断する。自分宛のデータでない場合には受信装置 2 は処理を終了する。宛先アドレスが自分宛のデータである場合には、ステップ S7 に進み、信号処理装置 21 は IP ヘッダ 14 を見て、暗号化データ 29 を復号鍵 8 を用いて復号するか否かを判断する。復号鍵 8 を用いて暗号化データ 29 を復号する場合にはステップ S8 に進み、信号処理装置 21 は復号器 9 において復号鍵 8 を用いた復号処理を行なわせ、その後、ステップ S9 においてデータを取り出す。ステップ S7 において復号鍵 8 を用いて復号しない場合には、ステップ S9 に進み、信号処理装置 21 は平文データ 28 を取り出す。

【0026】第 1 実施例の効果

映像・音声（AV）データ、あるいは、コンピュータデータなどの大容量のデータが衛星回線伝送路などの大容量伝送路 12 を介して、必要に応じて、暗号化されて伝送される。暗号化された AV データは公衆電話回線などの小容量伝送路 13 を介して事前に復号鍵 8 を送信装置 1 から送付されている受信装置 2 でしか有効に復号できない。したがって、図 2 に示した、有効に復号鍵 8 が授与されていない受信装置 3 において、仮に衛星回線伝送路 12 を介して暗号化データ 19 を受信したとしても意味のないデータを受信したことになり、実質的に第三者としての受信装置 3（図 2 参照）における盗聴（盗用）

が防止できる。暗号鍵7に対応する復号鍵8は公衆電話回線などの衛星回線伝送路に比較して機密性の高い有線の小容量伝送路13を介して伝送されるから、盗用者が大容量伝送路12のみ監視していても、復号鍵8は判らない。したがって第3者としての受信装置3（図2参照）において衛星回線伝送路12からのデータを受信したとしても、そのデータが暗号化されていれば、有効に復号できず、事実上、盗聴されたことにならない。特に、公衆電話回線などの小容量伝送路13は送信装置1と受信装置2との間で1対1の伝送を行う有線路であるから、盗聴を意図した受信装置3（図2参照）においては接続されず、衛星回線伝送路などの大容量伝送路12に比較して、盗聴または漏洩は起こりにくい。

【0027】

【実施例2】本発明のデータ伝送装置の第2実施例を述べる。図8は本発明の第2実施例としてのデータ伝送装置の概略構成図である。図8に図解したデータ伝送装置は、1台の送信装置1に対して2台の受信装置2A、2Bがそれぞれ衛星回線伝送路などの大容量伝送路（第1の伝送系統）12および公衆電話回線などの小容量伝送路（第2の伝送系統）13を介して接続されている。受信装置3は、図2に図解した場合と同様、送信装置1とは正規に接続しない受信装置3である。大容量伝送路12および小容量伝送路13の構成は、図3に図解した構成と同様である。第2実施例においては、送信装置1から2台の受信装置2A、2Bに対して小容量伝送路13を介して復号鍵（復号用セッションキー）と、大容量伝送路12を用いる伝送において使用する宛先アドレスを伝送する。受信装置2Aに対する宛先アドレスと受信装置2Bに対する宛先アドレスとは異なる。したがって、受信装置2Aまたは2Bは自己に対する伝送か否かを宛先アドレスを検査することによって識別できる。送信装置1と受信装置2A、または、送信装置1と受信装置2Bとのデータ伝送は、それぞれ、第1実施例と同じである。第2実施例によれば、大容量伝送路12を用いて、同時に複数、本実施例は2台の受信装置2A、2Bに暗号化データを伝送し、それぞれの受信装置で復号できる。もちろん、IPヘッダ14の伝送制御情報の暗号化するか否かを示すフラグがセットされていない場合は暗号化しないデータを伝送することもできる。

【0028】第2実施例の変形例

上述した第2実施例においては、2台の独立した宛先アドレスを有する受信装置2A、2Bが、同時に大容量伝送路12を介して暗号化データを受信でき、宛先アドレスが一致する受信装置が有効に暗号化データを復号する場合について述べたが、本実施例の変形態様としては、2台の受信装置2A、2Bの宛先アドレスを同じにして、2台の受信装置2A、2Bが同時に暗号化データを受信し、2台の受信装置の両方で暗号化データを復号可能にすることもできる。このような運用の例としては、

たとえば、ある企業の本社から複数の支部に同じ暗号化データを伝送する場合、複数の支店ごとに伝送することなく、1度で全ての支店に伝送する場合などがある。すなわち、伝送回数を少なくできるという利点がある。また、有料映像データを暗号化して多くの有料放送加盟者に伝送する場合なども、有料放送加盟者側の受信装置の宛先アドレスを同じにしておけば、それらの複数の受信装置に暗号化された有料映像データを1度伝送するだけで、有効な受信装置側で復号できる。

【0029】

【実施例3】本発明のデータ伝送装置の第3実施例を述べる。第3実施例のデータ伝送装置の構成は、図2、図5および図8を参照して述べた第1実施例および第2実施例のデータ伝送装置の構成と同様である。ただし、第1実施例および第2実施例においては、大容量伝送路12から暗号化データを伝送する前に、送信装置1から受信装置2に復号鍵（復号用セッションキー）を小容量伝送路13を介して伝送したが、第3実施例においては、受信装置2から送信装置1に小容量伝送路13を介して事前に暗号化鍵（暗号化用セッションキー）を伝送しておく。この暗号化鍵は、受信装置2において大容量伝送路12を用いたデータ伝送において使用する受信装置2の宛先アドレスに基づいて生成される。受信装置2において、暗号鍵に対応する復号鍵は判っている。送信装置1において伝送データを暗号化する場合には、この暗号化鍵を用いて暗号化処理を行う。暗号化データ伝送およびその復号処理は、第1実施例および第2実施例と同様である。第3実施例においては、受信装置2が送信装置1に対して暗号化鍵を指定することができる。

【0030】

【実施例4】本発明のデータ伝送装置の第4実施例を述べる。図9は本発明のデータ伝送装置の第4実施例の構成図である。送信装置1と受信装置2とは大容量伝送路12と小容量伝送路13を介して接続されている。これらの接続状態は図3に図解した接続状態と同様である。送信装置1は、小容量伝送路13に接続された変復調器（モデム）17、信号処理装置11、データ暗号化器6、IPデータグラム構成器16の他、キー暗号化器130およびキー変換器132を有している。キー暗号化器130は、マスターキー120とワークキー121から暗号化したキー123を生成する。暗号化したキー123が変復調器（モデム）17を経由して受信装置2の変復調器（モデム）27で受信される。IPデータグラム構成器16は伝送すべきデータ5に、暗号化伝送データの送信先である受信装置2の宛先アドレスおよび暗号化処理を行うか否かを示すフラグを有するIPヘッダ14を付加してIPデータグラム15を構成する。IPヘッダ14の宛先アドレスは、キー変換器132に入力され、ワークキー121とともにキー変換器132において暗号鍵（暗号化セッションキー）7を生成するのに使

用される。このように、暗号鍵7は、ワークキー121の他に、受信装置2の宛先アドレスを元にして生成されているので、正当な受信装置2以外で暗号化伝送データを受信したとしても、正当に復号できないことになる。この詳細は後述する。キー変換器132で生成された暗号鍵（セッションキー）7が暗号化器6において伝送すべきデータ5を暗号化するのに使用される。暗号化器6において暗号化され大容量伝送路12に送出されるデータが暗号化データ19である。暗号化データ19は、伝送すべきデータ5を暗号化したデータに、暗号化されていないIPヘッダ14が付加されて、図示しない送信手段によって大容量伝送路12に送出される。

【0031】受信装置2は、小容量伝送路13に接続された変復調器（モデム）27、信号処理装置21、IPデータグラム分解器26、データ復号器9の他に、キー復号器230、キー変換器232を有している。キー復号器230は変復調器（モデム）27を経由して受信した暗号化されているキー123をマスターキー220を用いてワークキー221を復号する。IPデータグラム分解器26は、暗号化データ19からIPヘッダ14を分離し、受信装置2の宛先アドレスを取り出し、キー変換器232に印加する。キー変換器232は、宛先アドレスと、復号されたワークキー221から復号鍵（復号用セッションキー）8を変換する。本実施例においては、宛先アドレスをも用いて復号鍵8を再生しているから、正当なアドレスでない受信装置においては正当な復号鍵が生成できない。なお、本実施例における宛先アドレスは単一の装置の宛先アドレスだけを意味するだけでなく、複数の受信装置から構成されるグループを意味（指定）することができる。その場合、上述した暗号化処理および復号処理は、複数の装置に対する暗号化処理および復号処理を意味する。キー変換器232で変換された復号鍵8は大容量伝送路12を経由して受信した暗号化データ19を復号するのに使用される。

【0032】送信装置1におけるマスターキー120と受信装置2におけるマスターキー220とは実質的に同じ内容である。マスターキー120を記録した物体を郵送する等して、送信装置1と受信装置2とでマスターキー120（220）を共有している。送信装置1はワークキー121を生成し、キー暗号化器130においてマスターキー120を鍵としてワークキー121を暗号化し、暗号化したキー123を変復調器（モデム）17を介して小容量伝送路13に送出し受信装置2に伝送する。また、ワークキー121をキー変換器132に入力して暗号鍵7に変換し、変換した暗号化鍵（暗号化用セッションキー）7を鍵として、データ暗号化器6において伝送すべきデータ5を暗号化して暗号化データ19として大容量伝送路12を介して受信装置2に伝送する。受信装置2において、小容量伝送路13から受信した暗号化したキー123をキー復号器230においてマスタ

ーキー220を用いてワークキー221を復号し、キー変換器232で復号鍵8に変換し、変換された復号鍵（復号用セッションキー）8を鍵としてデータ復号器9において大容量伝送路12から受信した暗号化データ19を復号する。

【0033】第4実施例のデータ伝送装置の送信装置1におけるワークキーの暗号化処理は、送信装置1と受信装置2の間で既に共有済みの受信装置2が持つ受信端末のシリアルナンバー等の固有情報を鍵（マスターキー）として行えば、受信装置2においてワークキーを得られるように行なわれる。

【0034】第4実施例においては、暗号化したキー123を小容量伝送路13を経由して伝送するから、ワークキーの漏洩があっても、マスターキー120を知らない限り復号鍵8が生成される可能性が殆どないので、鍵伝送の機密性が非常に高い。したがって、大容量伝送路12を伝送された暗号化データ19が第3者の受信装置3において正しく復号することが困難であり、情報の漏洩についても安全性がより高くなる。さらに第4実施例においては、送信先の受信装置2の宛先アドレスをも用いて暗号鍵7および復号鍵8の生成（変換）を行うので、正当な受信装置2でしか正当な暗号化器6を生成（再生）できず、かりに暗号化データ19を受信したとしても正常に暗号化データ19を復号できない。

【0035】第4実施例の第1変形例

図9には、好適実施例として、送信装置1においてワークキー121を暗号化して暗号化したキー123として受信装置2に伝送する例を示したが、第4実施例は、受信装置2の宛先アドレスを用いて暗号鍵7および復号鍵8を変換して機密性が高くなっているため、ワークキー121を小容量伝送路13を経由して直接、キー変換器232における復号鍵（復号化セッションキー）8の変換に使用してもよい。すなわち、図9に図解した送信装置1におけるキー暗号化器130、受信装置2におけるキー復号器230を削除することができる。この場合、マスターキー120、マスターキー220の交換をしなくて済むので、送信装置1と受信装置2との間の手続きは簡単になる。

【0036】第4実施例の第2変形例

また、図9を参照して述べた第4実施例は、好適実施例として、送信装置1におけるキー変換器132においてワークキー121と宛先アドレス14を用いて暗号化セッションキー7を変換し、その暗号化セッションキー7を用いてデータ15を暗号化器6において暗号処理する場合を述べたが、第4実施例の簡便な例として、キー変換器132において、宛先アドレス14を用いず、ワークキー121のみを用いて暗号化鍵（暗号化セッションキー）7を生成することができる。この場合、キー変換器132の構成が簡単になる。同様に、受信装置2におけるキー変換器232においても、マスターキー120

と同じマスターキー 220 を用いて復号鍵（復号セッションキー）8 を生成して、その復号鍵 8 を用いて受信した暗号化データを復号できる。この場合も、キー変換器 232 の構成が簡単になる。

【0037】第4実施例の第3変形例

さらに、上述した第4実施例の第1の変形例と第2変形例を組み合わせることもできる。すなわち、第4実施例の第1変形例に従って、図9に図解した送信装置1におけるキー暗号化器130、受信装置2におけるキー復号器230を削除し、第2変形例に従って、キー変換器132およびキー変換器232の構成を簡単にする。

【0038】

【実施例5】本発明のデータ伝送装置の第5実施例を述べる。図10は本発明のデータ伝送装置の第5実施例の構成図である。第4実施例においては、小容量伝送路13を用いて、送信装置1から受信装置2に暗号化したキー123を送信したが、第5実施例は、1台の受信装置2が存在しただけのとき、受信装置2から送信装置1に暗号化したワークキー223を小容量伝送路13を経由して伝送し、送信装置1において、暗号化したワークキー223からワークキー121を復号し、このワークキー121から暗号鍵7を変換する。このため、送信装置1には、図9に図解したキー暗号化器130に代えてキー復号器230と同等のキー復号器134が設けられ、受信装置2には、図9に図解したキー暗号化器130と同等のキー暗号化器234が設けられている。その他の構成および動作は第4実施例と同様である。第5実施例においては、送信装置1に対して受信装置2から暗号化鍵（暗号化用セッションキー）を指定することができる。第5実施例における鍵の機密性、暗号化データ19の機密性は第4実施例と同等である。

【0039】第5実施例の変形例

図10には、好適実施例として、送信装置1においてワークキー121を暗号化して暗号化したキー123として受信装置2に伝送する例を示したが、第5実施例は、第4実施例と同様、受信装置2の宛先アドレスを用いて暗号鍵7および復号鍵8を変換して機密性が高いので、ワークキー221を小容量伝送路13を経由して直接、送信装置1のキー変換器132における暗号鍵7の変換に使用してもよい。すなわち、送信装置1におけるキー復号器134、受信装置2におけるキー暗号化器234を削除することができる。この場合、マスターキー120、マスターキー220の交換をしないで済むので、手続きは簡単になる。その他、第5実施例についても、第4実施例の変形例として述べた種々の簡単な構成をとることができる。

【0040】

【実施例6】本発明のデータ伝送装置の第6実施例を述べる。第4実施例および第5実施例においては、送信装置1および受信装置2において、好適には、ワークキー

121と宛先アドレスから、簡便には、第4実施例の変形例として述べたように、ワークキー121から暗号鍵（暗号用セッションキー）7を変換するためのキー変換器132、および、ワークキー221から復号鍵（復号用セッションキー）8を変換するためのキー変換器232を設けている。これに対して第6実施例においては、送信装置1のキー変換器132の入力を、ワークキー121と大容量伝送路12を用いる伝送における宛先アドレスとし、これらの情報から暗号鍵（暗号用セッションキー）7を生成する。同様に、受信装置2のキー変換器232の入力を、ワークキー221と受信装置2のアドレスとし、これらの情報から復号鍵（復号用セッションキー）7を生成する。その他の構成および動作は第4実施例と同様である。なお、第6実施例においても、宛先アドレスは単一の装置の宛先アドレスだけを意味するだけでなく、複数の受信装置から構成されるグループを意味（指定）することができる。その場合、上述した暗号化処理および復号処理は、複数の装置に対する暗号化処理および復号処理を意味する。第6実施例においては、第4実施例のようにワークキーのみからセッションキーを生成する方法に対して、宛先アドレスを知らない者にはセッションキーを生成することが困難であるから、鍵の伝送の安全性がより高くなるという利点がある。

【0041】

【実施例7】本発明のデータ伝送装置の第7実施例を述べる。図11は本発明のデータ伝送装置の第7実施例の構成図である。データ伝送装置は、大容量伝送路12および小容量伝送路13を介して接続される送信装置1と受信装置2とを有する。送信装置1は、暗号化器6およびキー暗号化器136を有する。受信装置2は復号器9およびキー復号器236を有する。なお図解を簡単するため、図11には図5に示したIPデータグラム構成器16およびIPデータグラム分解器26は図示していない。しかしながら、本実施例においても、IPヘッダ14に規定されている宛先データの処理および暗号処理を行うか否かの処理は上述した実施例と同様に行う。

【0042】第4実施例では送信装置1から受信装置2に暗号化したキー123を小容量伝送路13を用いて伝送し、第5実施例では受信装置2から送信装置1に暗号化したワークキー223を小容量伝送路13を用いて伝送している。これに対して第7実施例では、送信装置1から受信装置2に暗号化したセッションキー124を小容量伝送路13を用いて伝送する。また、受信装置2が1台の場合は、受信装置2から送信装置1に暗号化したセッションキーを小容量伝送路13を用いて伝送する。このセッションキーは、大容量伝送路12を用いた暗号化データ伝送における宛先アドレスに基づいて生成される。

【0043】送信装置1において暗号化用鍵（暗号化用セッションキー）7を生成し、送信装置1と受信装置2

において共有するマスターキー 120 を鍵としてキー暗号化器 136 を用いて暗号化し、暗号化されたセッションキー 124 を小容量伝送路 13 を用いて受信装置 2 に送る。送信装置 1 においては、生成した暗号化鍵 7 を鍵として暗号化器 6 を用いて伝送すべきデータ 5 を暗号化して大容量伝送路 12 を用いて受信装置 2 に送る。受信装置 2 は小容量伝送路 13 から受信した暗号化されたセッションキー 124 をマスターキー 220 を鍵として復号器 9 で復号し、復号鍵（復号用セッションキー）8 を得る。受信装置 2 において、大容量伝送路 12 から受信した暗号化データ 19 を、上記のようにして求めた復号鍵 8 を鍵として復号器 9 で復号する。第 7 実施例は、直接、暗号化したセッションキー 124 を送信装置 1 から受信装置 2 に伝送しているの、送信装置 1 および受信装置 2 におけるキー変換器 132 およびキー変換器 232 が不要であるという構成上の利点がある。

【0044】

【実施例 8】本発明のデータ伝送装置の第 8 実施例を述べる。図 12 は本発明のデータ伝送装置の第 8 実施例の構成図である。送信装置 1 は IP データグラム構成器 16 および暗号化器 6 を有する。受信装置 2 は復号器 9 および IP データグラム分解器 26 を有する。送信装置 1 において、伝送すべきデータ 5 が IP データグラム構成器 16 に入力されて IP ヘッダ 14 が付加されて IP データグラム 15 が形成される。暗号化器 6 は IP ヘッダ 14 に含まれる宛先データも暗号化する。IP ヘッダ 14 のデータも暗号化したデータ 19 が大容量伝送路 12 を経由して受信装置 2 に伝送される。受信装置 2 は、大容量伝送路 12 から受信した IP ヘッダ 14 のデータも暗号化したデータ 19 の全てを復号器 9 において復号する。それにより、IP データグラム 15 も復号される。IP データグラム分解器 26 が復号した IP データグラム 15 を分解して IP ヘッダ 14 を取り出し、この中の宛先アドレスを見て、それが自分宛のデータであるか否かを知り、自分宛のデータである場合には、IP ヘッダを取り除いたもののデータ部分を取り出す。なお、本実施例において、小容量伝送路 13 を用いた送信装置 1 と受信装置 2 との間の暗号鍵または暗号鍵を生成するための情報の授受、あるいは、送信装置 1 と受信装置 2 との間で復号鍵または復号鍵を生成するための情報の授受は、上述した第 1 ～第 7 実施例のいずれも適用できる。すなわち、本実施例は、IP ヘッダ 14 も暗号化の対象にした例を示しており、小容量伝送路 13 を用いた暗号鍵または復号鍵の伝送方法は上述した実施例のいずれも適用できる。本実施例においては、送信装置 1 または受信装置 2 において、伝送されているデータを暗号化あるいは復号するかしないかの判断を省略することができる。

【0045】変形例

上述した実施例は全て、インターネット・プロトコル I

P を用いた場合について例示したが、本発明の実施に際しては、インターネット・プロトコル IP に限定されず、その他の伝送プロトコル、たとえば、ATM (Asynchronous Transfer Mode、非同期転送モード) に従うプロトコルなどを用いることができる。また本発明の実施に際しては、上述した種々の実施例を適宜組み合わせることができる。

【0046】

【発明の効果】本発明によれば、データを伝送する大容量伝送路（第 1 の伝送系統）とは異なる小容量伝送路（第 2 の伝送系統）を用いて暗号化あるいは復号の処理のための鍵あるいはこの鍵を生成するための情報を伝送して鍵の伝送の機密性を高めており、大容量伝送路を介して伝送される暗号化データの漏洩に対して安全性が高くなる。特に、本発明においては、制御情報として宛先データを付加しているの、正当な受信装置（第 2 の伝送装置）においてのみ有効に暗号化データが復号可能となる。また本発明においては、鍵を暗号化して伝送できるので、鍵の漏洩に対する安全性が一層高まる。

【0047】また本発明によれば、伝送のために必要な制御情報を見るだけで暗号化、復号の必要性が判別できる。

【図面の簡単な説明】

【図 1】図 1 は伝送路上のデータを暗号化する伝送方法の一例を示す概略図である。

【図 2】図 2 は本発明のデータ伝送装置の第 1 実施例の構成を示す概略図である。

【図 3】図 3 は本発明の実施例のデータ伝送装置における大容量伝送路および小容量伝送路の具体的構成を示す図である。

【図 4】図 4 はインターネット・プロトコル IP におけるメッセージ伝送の単位である IP データグラムの概略図である。

【図 5】図 5 は図 2 に図解した本発明のデータ伝送装置の第 1 実施例についてインターネット・プロトコル IP を適用して実現したより詳細な構成を示す図である。

【図 6】図 6 は本発明のデータ伝送装置の実施例における送信装置の動作処理を示すフローチャートである。

【図 7】図 7 は本発明のデータ伝送装置の実施例における受信装置の動作処理を示すフローチャートである。

【図 8】図 8 は本発明のデータ伝送装置の第 3 実施例の概略構成図である。

【図 9】図 9 は本発明のデータ伝送装置の第 4 実施例の構成図である。

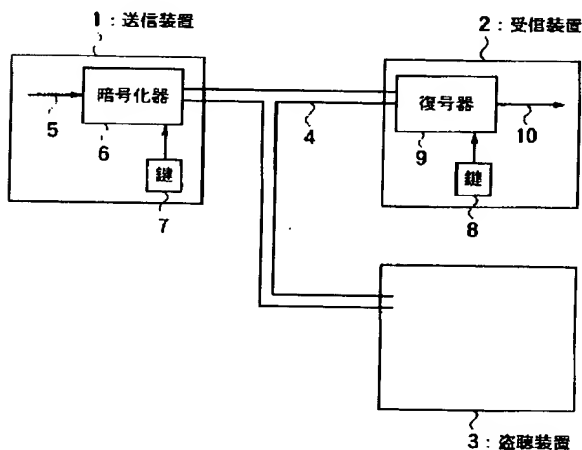
【図 10】図 10 は本発明のデータ伝送装置の第 5 実施例の構成図である。

【図 11】図 11 は本発明のデータ伝送装置の第 7 実施例の構成図である。

【図 12】図 12 は本発明のデータ伝送装置の第 8 実施例の構成図である。

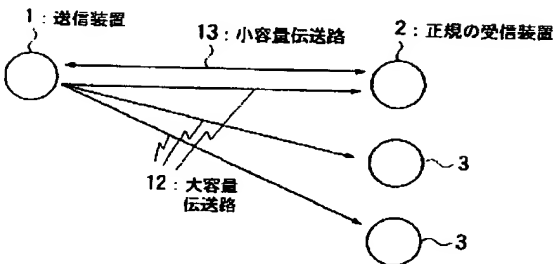
- 【符号の説明】
- 1・・・送信者 2・・・受信者 3・・・盗聴受信装置
 - 5・・・伝送すべきデータ
 - 6・・・暗号化器 7・・・暗号鍵（暗号化用セッションキー）
 - 8・・・復号鍵（復号化用セッションキー）
 - 9・・・復号器
 - 12・・・大容量伝送路（衛星回線伝送路）
 - 13・・・小容量伝送路（公衆電話回線）

【図 1】

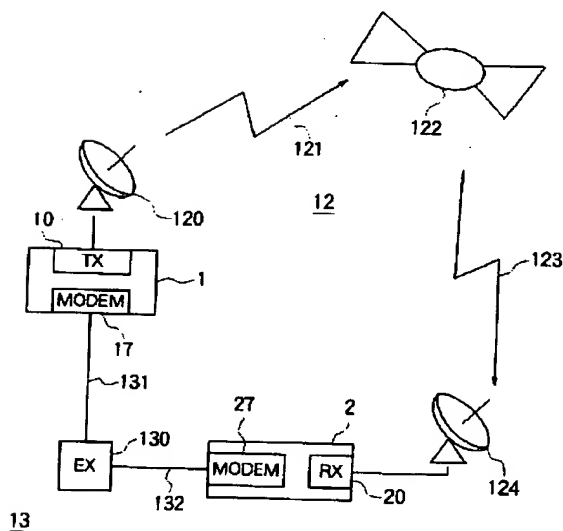


- * 14・・・IPヘッダ
- 15・・・IPデータグラム
- 16・・・IPデータグラム構成器 26・・・IPデータグラム分解器
- 17、27・・・変復調器（モデム）
- 19・・・暗号化データ
- 120、220・・・マスターキー
- 121、221・・・ワークキー
- * 123、223・・・暗号化したキー

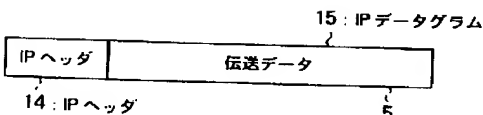
【図 2】



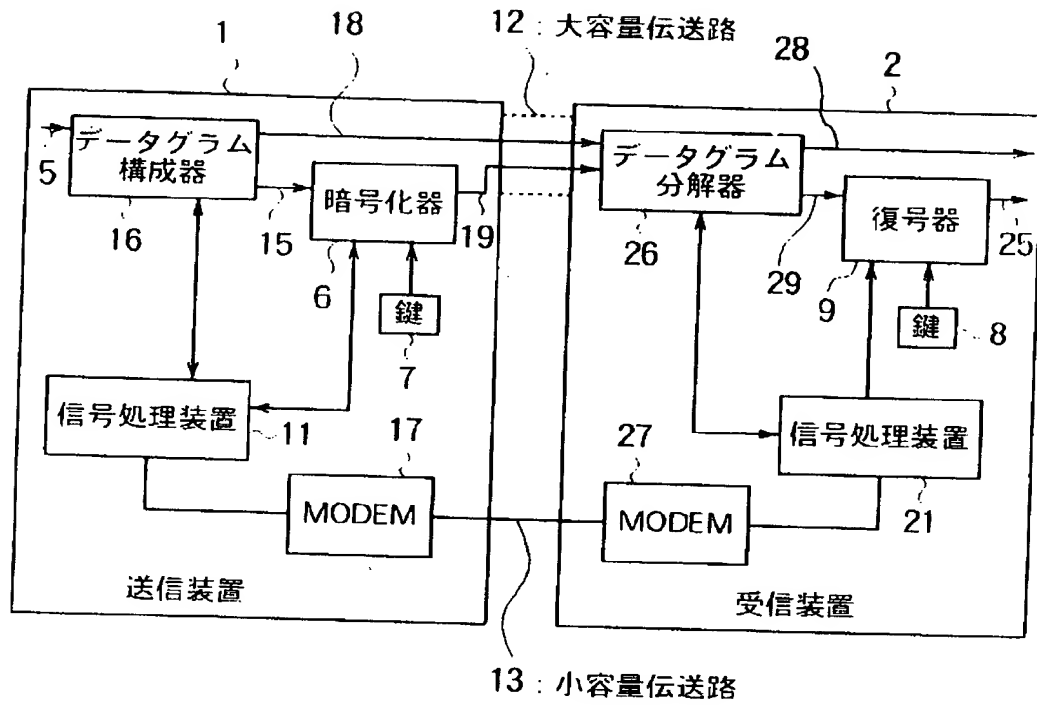
【図 3】



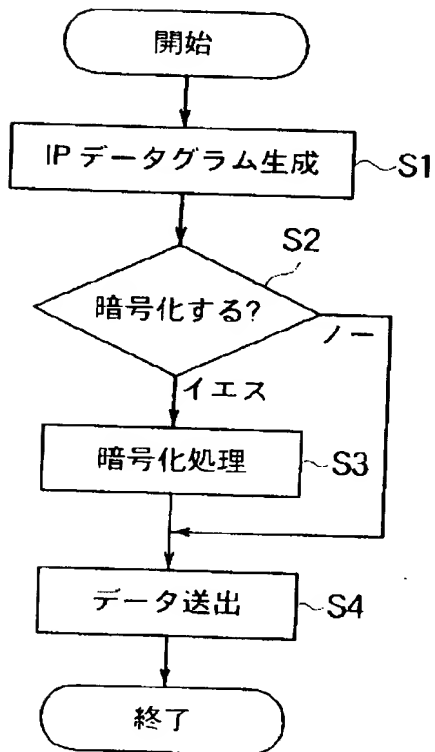
【図 4】



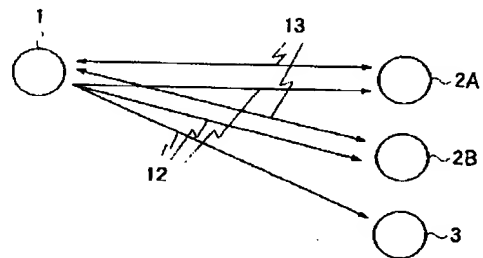
【図5】



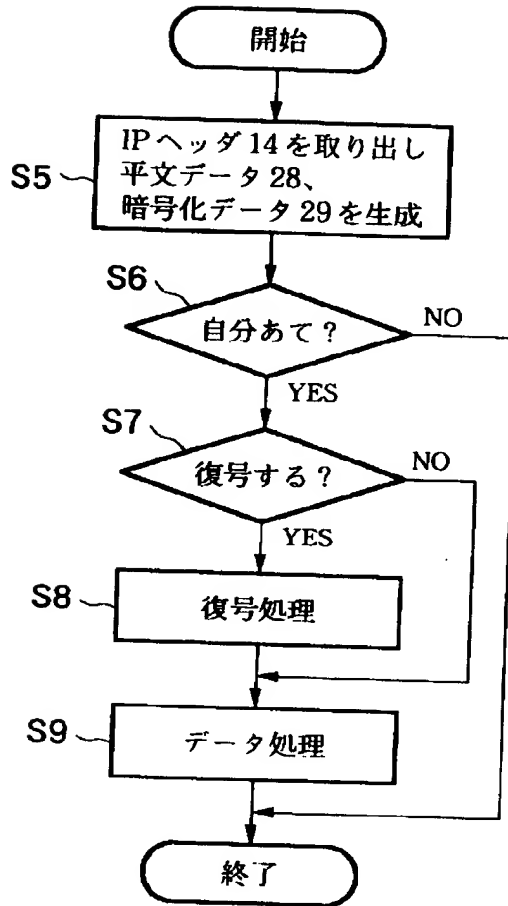
【図6】



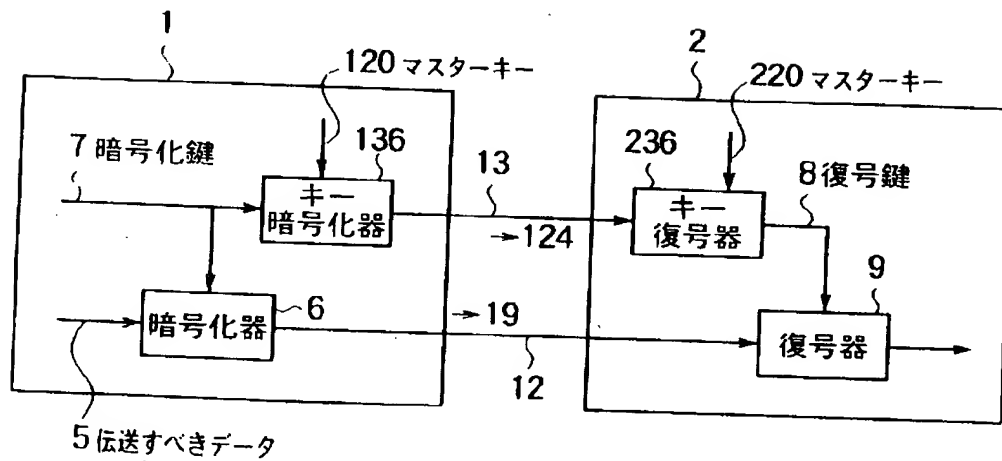
【図8】



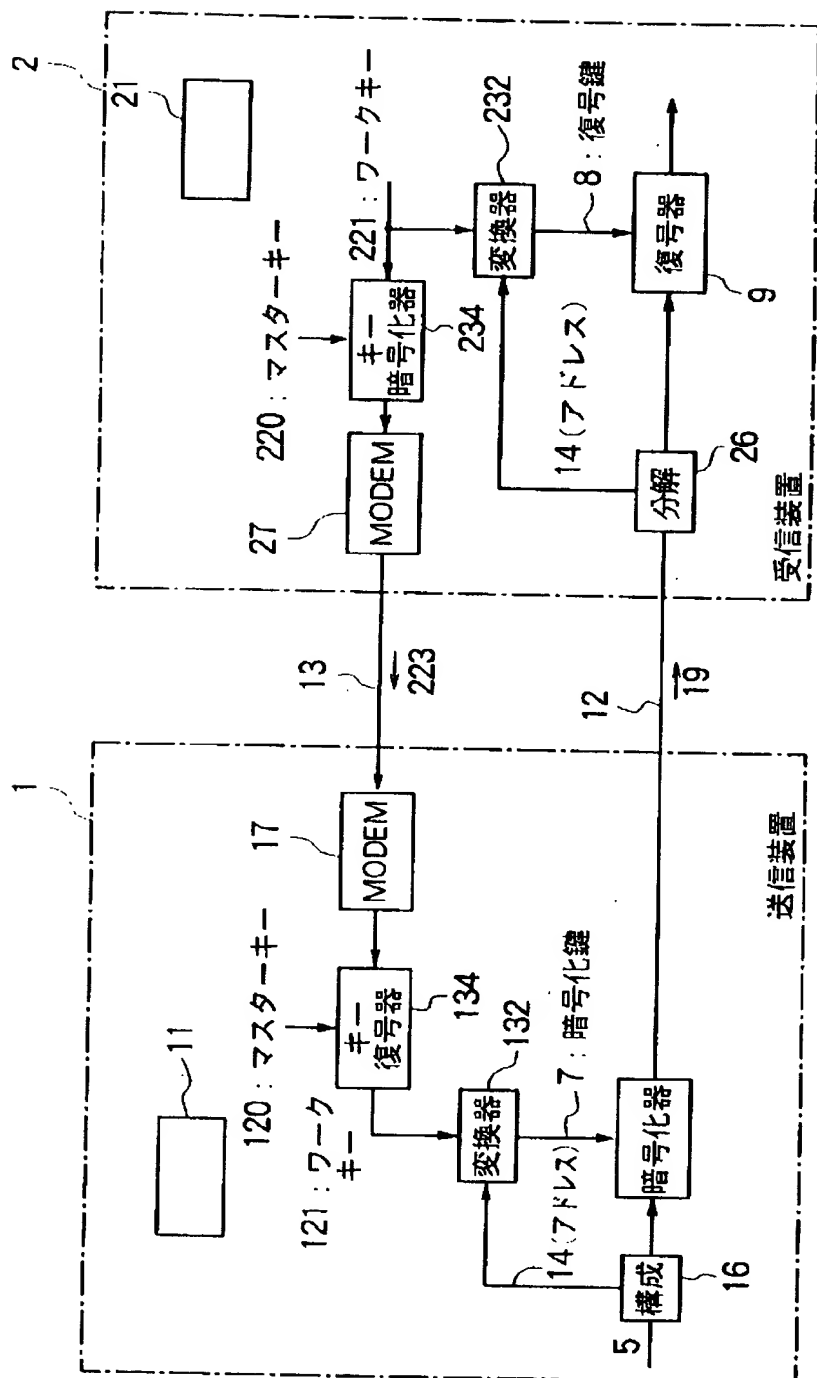
【図7】



【図11】



【図10】



【図12】

